PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-101545

(43)Date of publication of application : 04.04.2003

(51)Int.Cl. H04L 12/28

(21)Application number : 2001-285854

(22)Date of filing : 19.09.2001

(71)Applicant : HITACHI SOFTWARE ENG CO LTD

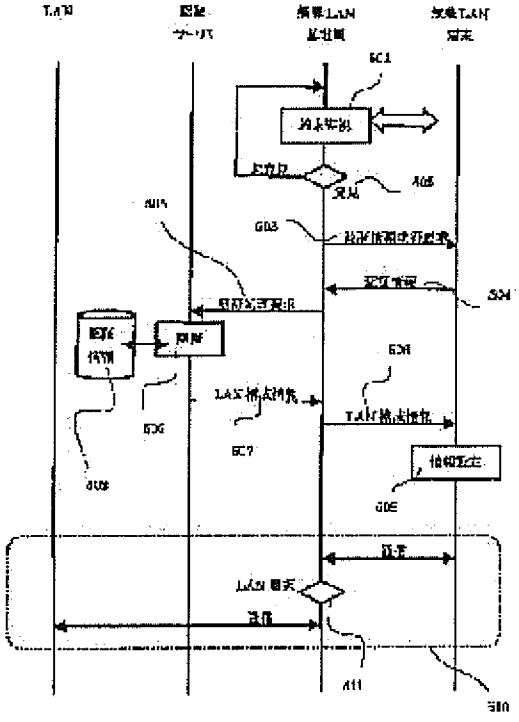
(72)Inventor : IKETANI SEIICHIRO
TAKAHASHI HIROAKI

(54) METHOD FOR CONTROLLING ACCESS TO LAN FROM WIRELESS LAN TERMINAL, WIRELESS LAN BASE STATION APPARATUS AND WIRELESS LAN TERMINAL APPARATUS

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for controlling access to a LAN from a wireless LAN terminal, a wireless LAN base station apparatus and a wireless LAN terminal apparatus enabling the wireless LAN terminal apparatus to access wirelessly to the LAN without threatening security of resources in the LAN.

SOLUTION: A method comprises a step in which a base station detects a wireless LAN terminal entering within the range of electric waves emitted from the wireless base station itself, and obtains authentication information from a wireless tag given to the wireless LAN terminal, a step to check the obtained authentication information against authentication information registered in the wireless base station or in an authentication device connected with the wireless base station, and determine if the wireless LAN terminal is allowed to access one of a plurality of wireless LANs, and a step to transmit configuration information of the plurality of wireless LANs registered in the wireless base station, or obtained from the external device connected to the wireless base station to the wireless LAN terminal in accordance with the decision result.



LEGAL STATUS

[Date of request for examination]	17.05.2004
[Date of sending the examiner's decision of rejection]	14.07.2006
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3865317
[Date of registration]	13.10.2006
[Number of appeal against examiner's decision of rejection]	2006-017310
[Date of requesting appeal against examiner's decision of rejection]	09.08.2006
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It is the approach of controlling said wireless LAN terminal possible [connection] to either of two or more wireless LAN which detects the wireless LAN terminal which invaded into electric-wave attainment within the limits of a base transceiver station, and uses the same frequency band identically within the area. The step which acquires authentication information from the wireless components which detected the wireless LAN terminal which invaded into electric-wave attainment within the limits of self-equipment in said base transceiver station, and were added to the wireless LAN terminal concerned, The authentication information acquired from the authentication equipment connected with the authentication information or the base transceiver station set up in the base transceiver station and the authentication information acquired from said wireless component are collated. The step which judges whether connection with either of two or more wireless LAN is permitted, The step which transmits the configuration information of two or more wireless LAN acquired from the external device connected with the configuration information of two or more wireless LAN or the base transceiver station set up in the base transceiver station based on the judgment result of connection authorization to said wireless LAN terminal, The participating control approach to the wireless LAN of the wireless LAN terminal characterized by having the step whose connection with either of two or more wireless LAN sets up said wireless LAN configuration information received from said base transceiver station in the wireless LAN terminal within the end of a local, and is enabled according to the wireless LAN configuration information concerned.
[Claim 2] It is equipment which controls said wireless LAN terminal possible [connection] to either of two or more wireless LAN which detects the wireless LAN terminal which invaded into electric-wave attainment within the limits of self-equipment, and uses the same frequency band identically within the area. A means to acquire authentication information from the wireless components which detected the wireless LAN terminal which invaded into electric-wave attainment within the limits of self-equipment, and were added to the wireless LAN terminal concerned, A means to judge whether the authentication information acquired from the authentication equipment connected with the authentication information or self-equipment set up in self-equipment and the authentication information acquired from said wireless component are collated, and connection with either of two or more wireless LAN is permitted, Wireless LAN base station equipment which transmits the configuration information of two or more wireless LAN acquired from the external device connected with the configuration information of two or more wireless LAN or self-equipment set up in self-equipment based on the judgment result of connection authorization to said wireless LAN terminal, and is characterized by having a means to set up.
[Claim 3] Wireless LAN base station equipment according to claim 2 characterized by having a means to distribute the communication link to two or more wireless LAN from a wireless LAN terminal based on the protocol of the high order of a radio protocol with a wireless LAN terminal.
[Claim 4] It is the wireless LAN terminal unit controlled by the connectable condition to either of two or more wireless LAN which uses the same frequency band identically within the area based on the control

from a base transceiver station. The wireless components which answer a letter by wireless in the authentication information on self-equipment according to the demand from said base transceiver station, The wireless LAN terminal unit characterized by having the means whose connection with either of two or more wireless LAN receives the wireless LAN configuration information transmitted from said base transceiver station according to the authentication processing in said base transceiver station, and sets up in self-equipment, and is enabled according to the wireless LAN configuration information concerned.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention detects the wireless LAN terminal which invaded into electric-wave attainment within the limits of a base transceiver station, and relates to a wireless LAN terminal unit at the approach and wireless LAN base station equipment list which control said wireless LAN terminal possible [connection] to either of two or more wireless LAN which uses the same frequency band identically within the area.
[0002]
[Description of the Prior Art] The wireless LAN terminal which a wireless LAN base station exists on one network of a LAN (Local Area Network) protocol, and communicates with the same wireless LAN base station in a wireless LAN system can be connected only with the wireless LAN which the wireless LAN base station has connected. A wireless LAN base station is equipped with a wireless interface and every one LAN interface, and exchange of a wireless protocol and a LAN protocol is performed by passing both communication links transparent. For this reason, an interface is set to 1:1 and serves as connection with one LAN to one radio frequency band.
[0003] Moreover, when a wireless LAN terminal connects with wireless LAN through a wireless LAN base station, after configuration information, such as a network address of the wireless LAN (or it participates) to connect, comes to hand beforehand, processing set as the interior of the wireless LAN terminal itself is performed, and connection with a wireless LAN base station and connection with wireless LAN are made. Moreover, authentication processing which it permits using the resource on wireless LAN is performed between a wireless LAN terminal and the authentication equipment currently installed on wireless LAN, after connection with wireless LAN is made. Only authentication is performed, after this is performed on LAN protocols, such as TCP/IP, and is in the condition in which a fundamental communication link is possible.
[0004]
[Problem(s) to be Solved by the Invention] By the way, at office or works, two or more wireless LAN doubled not only with single wireless LAN but with the application is laid in many cases. According to the laid wireless LAN, it is necessary to install two or more wireless LAN base stations in such an environment. On the other hand, the user of the wireless LAN terminal to connect needs to receive in advance the LAN configuration information (a network address, subnet mask, etc.) doubled with the wireless LAN of a connection place, and needs to perform a setup on a terminal.
[0005] However, since it becomes possible to access the resource of the fixed range on wireless LAN, making the user of a wireless LAN terminal receive the configuration information of wireless LAN beforehand becomes the cause which causes unlawful access of a resource, and it has the problem on management of a resource, or a security management of not being desirable. Moreover, configuration information, such as a network address, is given according to the fixed Ruhr in many cases, disclosing the configuration information on wireless LAN shows that an analogy of other equipment configurations on wireless LAN is attained, and this also has the problem of not being desirable, in respect of a security

management.
[0006] On the other hand, since configuration information cannot come to hand when a manager is absent if the user of a wireless LAN terminal who expects connection of wireless LAN temporarily has it, although the configuration information of wireless LAN is managed by the manager in many cases, there is a problem that use is impossible temporarily. Moreover, although attested in a connection phase by the remote access by LAN using public lines, such as a telephone, at wireless LAN, it is rare to perform authentication on the connection level which makes a communication link possible, configuration information is set up, and connection with wireless LAN is attained by making connection with a wireless LAN base station in many cases. However, on wireless LAN, since the resource which can be accessed even if it does not attest also exists, by the authentication processing after connection, the problem of it becoming impossible to secure sufficient security is.
[0007] It is made in order that this invention may solve such a problem, and the 1st purpose is in providing with a wireless LAN terminal unit the participating control approach to LAN of the wireless LAN terminal which enables connection of a wireless LAN terminal, and a wireless LAN base station equipment list, without threatening safeties, such as a resource in wireless LAN. The 2nd purpose of this invention is to provide with a wireless LAN terminal unit the participating control approach to the wireless LAN of the wireless LAN terminal which enables connection of a wireless LAN terminal unit alternatively by one wireless LAN base station at either of two or more wireless LAN, and a wireless LAN base station equipment list.
[0008]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, the participating control approach to the wireless LAN of the wireless LAN terminal of this invention It is the approach of controlling said wireless LAN terminal possible [connection] to either of two or more wireless LAN which detects the wireless LAN terminal which invaded into electric-wave attainment within the limits of a base transceiver station, and uses the same frequency band identically within the area. The step which acquires authentication information from the wireless components which detected the wireless LAN terminal which invaded into electric-wave attainment within the limits of self-equipment in said base transceiver station, and were added to the wireless LAN terminal concerned, The authentication information acquired from the authentication equipment connected with the authentication information or the base transceiver station set up in the base transceiver station and the authentication information acquired from said wireless component are collated. The step which judges whether connection with either of two or more wireless LAN is permitted, The step which transmits the configuration information of two or more wireless LAN acquired from the external device connected with the configuration information of two or more wireless LAN or the base transceiver station set up in the base transceiver station based on the judgment result of connection authorization to said wireless LAN terminal, Said wireless LAN configuration information received from said base transceiver station in the wireless LAN terminal is set up within the end of a local, and it is characterized by having the step whose connection with either of two or more wireless LAN is enabled according to the wireless LAN configuration information concerned.
[0009] The wireless LAN base station equipment of this invention detects the wireless LAN terminal which invaded into electric-wave attainment within the limits of self-equipment. It is equipment which controls said wireless LAN terminal possible [connection] to either of two or more wireless LAN which uses the same frequency band identically within the area. A means to acquire authentication information from the wireless components which detected the wireless LAN terminal which invaded into electric-wave attainment within the limits of self-equipment, and were added to the wireless LAN terminal concerned, A means to judge whether the authentication information acquired from the authentication equipment connected with the authentication information or self-equipment set up in self-equipment and the authentication information acquired from said wireless component are collated, and connection with either of two or more wireless LAN is permitted, Based on the judgment result of connection authorization, the configuration information of two or more wireless LAN acquired from the external device connected with the configuration information of two or more wireless LAN or self-

equipment set up in self-equipment is transmitted to said wireless LAN terminal, and it is characterized by having a means to set up. Moreover, it is characterized by having a means to distribute the communication link to two or more wireless LAN from a wireless LAN terminal based on the protocol of the high order of a radio protocol with a wireless LAN terminal.
[0010] Moreover, the wireless LAN terminal unit concerning this invention is based on control from a base transceiver station. The wireless components which are the wireless LAN terminal units controlled by the connectable condition to either of two or more wireless LAN which uses the same frequency band identically within the area, and answer a letter by wireless in the authentication information on self-equipment according to the demand from said base transceiver station, The wireless LAN configuration information transmitted from said base transceiver station according to the authentication processing in said base transceiver station is received, and it sets up in self-equipment, and is characterized by having the means whose connection with either of two or more wireless LAN is enabled according to the wireless LAN configuration information concerned.
[0011]
[Embodiment of the Invention] Hereafter, one gestalt in the case of carrying out this invention is concretely explained based on a drawing. Drawing 1 is the system configuration Fig. showing the operation gestalt of this invention. This invention consists of two or more wireless LAN terminals 104A and 104B which make a communication link possible with the wireless LAN base station 101 which controls two or more LAN 102A-102C held in the base station 101 of the wireless LAN which built or connected [external] the antenna, and this one wireless LAN base station 101, the authentication server 103 for attesting whether the participation to these LANs 102A-102C is allowed, and connection with LANs 102A-102C. The transmitter-receivers 105A-105C with which two or more LAN 102A-102C communicates by the wireless circuit between the wireless LAN base stations 101 are connected. By having connected these transmitter-receivers 105A-105C, the function as wireless LAN which uses the same frequency band identically [LANs 102A-102C] within the area is added.
[0012] On the other hand, the wireless LAN base station 101 detects the wireless LAN terminals 104A and 104B which invaded into electric-wave attainment within the limits of a local station 101. Authentication information is acquired from the detected wireless LAN terminal 104A104B by the wireless circuit. If the acquired authentication information is transmitted to an authentication server 102 by wireless or the wire circuit, authentication processing of whether to permit connection with LANs 102A-102C is performed and the response of Authentication O.K. is obtained The configuration information of LANs 102A-102C is transmitted to the LAN terminals 104A and 104B. At the LAN terminals 104A and 104B which received the configuration information of LANs 102A-102C, the configuration information is registered into the memory in self-equipment, and it communicates by emitting a connection request to either of LANs 102A-102C with reference to the contents of registration.
[0013] The wireless tags (wireless components) 106A and 106B with which the authentication information for connecting with LANs 102A-102C was registered into the wireless LAN terminals 104A and 104B are added to some cases. The authentication information registered into these wireless tags 106A and 106B answers an inquiry signal from the wireless LAN base station 101, and is answered to the wireless LAN base station 101. These wireless tags 106A and 106B contain an indirectional antenna, a cell, and LSI memory, and answer a letter considering the authentication information registered as a reply signal according to the inquiry signal from the wireless LAN base station 101.
[0014] Drawing 2 is drawing having shown the example of a detail configuration of wireless LAN terminal 104A. Wireless LAN terminal 104A consists of processing units 1042 which perform processing of the data which communicated with the transceiver antenna 1041 for performing the communication link with the wireless LAN base station 101, and analysis, and wireless tag 106A is attached in some cases. The LAN configuration information setting field 1043 for holding the configuration information for connecting with LANs 102A-102C transmitted to a processing unit 1042 from the wireless LAN base station 1011 is secured in memory. The information set as this LAN configuration information setting field 1043 holds the configuration information which enables

connection with LANs 102A-102C other than the configuration information which makes wireless connection. Generally, TCP/IP is used and information, such as an IP address, a network address, the gateway address, and various server addresses, is the contents of LAN configuration information.
[0015] On the other hand, the authentication information registered into wireless tag 106A is the authentication information for participating in LANs 102A-102C, and consists of unique identifiers and passwords for specifying self-equipment 104A at worst. Drawing 3 is drawing having shown the example of a detail configuration of the wireless LAN base station 101. The wireless LAN base station 101 has the function of exchange of the invasion monitor of the wireless LAN terminal which is the function which the base station in the former has, and a not only the radio between LANs but a wireless LAN terminal, front [connection] authentication processing, and the communication link between LANs.
[0016] The wireless LAN base station 101 of this example has the processing control unit 1011 which takes the lead in functions, such as a communication link and authentication, and is constituted from a LAN communication link exchange style 1012 which controls radio, and an authentication controlling mechanism 1013 which performs control of authentication by the processing control unit 1011. In the processing control unit 1011, it has the LAN transceiver antenna 1014 which communicates with the transmitter-receivers 105A-105C of LANs 102A-102C used as the candidate for a communication link, and the terminal transceiver antenna 1015 which performs the communication link with the wireless LAN terminals 104A and 104B. Moreover, the wireless LAN base station 101 has the authentication server connection interface 1016 for connecting with an authentication server 103.
[0017] The wireless LAN base station 101 sends out the electric wave for terminal detection at intervals of predetermined time from the terminal transceiver antenna 1015. When [which was supervising and invaded] it detects, whether one of wireless LAN terminals invaded into electric-wave attainment within the limits of a local station Authentication information is acquired from the wireless tags 106A or 106B of the detected wireless LAN terminal, the acquired authentication information is transmitted to an authentication server 103 by processing of the authentication controlling mechanism 1013, and authentication processing is performed. If the response of Authentication O.K. is answered from an authentication server 103, configuration information, such as a network address of LAN102A102C, will be acquired from an authentication server 103, you will transmit to the wireless LAN terminal which detected invasion, and the LAN configuration information setting field 1403 of the wireless LAN terminal will make it set up.
[0018] Thereby, the wireless LAN terminals 104A or 104B which invaded into electric-wave attainment within the limits of the wireless LAN base station 101 become connectable with either 102A-102C through the wireless LAN base station 101. In this case, LANs 102A-102C used as the candidate for connection analyze higher-level protocol information, such as TCP/IP, at LAN communication link exchange guard 1012, and are chosen according to that analysis result. It means that the wireless LAN system which multiplexed and held two or more LANs in one wireless LAN base station as the whole by connection distribution processing to two or more LANs which can be set to such one wireless LAN base station 101 was built.
[0019] Drawing 4 is the wireless LAN terminals 104A and 104B and the explanatory view of the LAN connection authentication processing performed between authentication servers 103. Although the wireless LAN base station 101 is monitoring invasion of the wireless LAN terminals 104A and 104B into the electric-wave area of influence of a local station continuously, if invasion is detected, it will perform authentication processing between the wireless LAN base station 101, the wireless LAN terminals 104A and 104B, and an authentication server 103. The wireless tags 106A and 106B holding the authentication information 401 which consists of user ID 4011 and a password 4012 at least are added to the wireless LAN terminals 104A and 104B. User ID 4011 is the information for specifying uniquely the wireless LAN terminals 104A and 104B, and serves as key information for searching the data on an authentication server 103. A password 4012 is collated with the password on an authentication server 103, and is used as that by which the authentication information on wireless LAN terminal 104A and 104B was registered into normal, or information for (connection with LAN would

not be permitted by normal), and identifying.
[0020] It is held at the authentication server 103 so that the LAN configuration information 4022 to which connection with LANs 102A-102C is permitted for a password 4021 and connection can be retrieved for user ID as a key. The wireless LAN base station 101 transmits the user ID 4011 of the authentication information 401 acquired from the wireless LAN terminals 104A or 104B which detected invasion, and a password 4012 to an authentication server 103. The authentication information 402 currently held inside is retrieved in an authentication server 103 by using user ID 4011 which received as a key. When corresponding authentication information is held, a password 4012 is collated and it checks that it is in agreement. When in agreement, it considers as an authentication success and the wireless LAN base station 101 is answered by making into an authentication result LAN configuration information 4022 retrieved by user ID 4011.
[0021] The wireless LAN base station 101 is transmitted to the wireless LAN terminals 104A or 104B which carried out invasion detection of the answered LAN configuration information 4022. On the other hand, the received LAN configuration information 4022 is registered into the LAN configuration information setting field 1403 at the wireless LAN terminals 104A or 104B. Thereby, the participation to LANs 102A-1025C is attained using the LAN configuration information 4022. In this case, since it can set up for every user ID so that the contents of the LAN configuration information 4022 may be differed, it is controllable by the user whether it is connectable with any of LANs 102A-102C.
[0022] In addition, when it becomes authentication failure, an error response is transmitted to the corresponding wireless LAN terminal, and LAN configuration information is not transmitted. Therefore, the participation to LANs 102A-12C becomes impossible, and except the wireless LAN terminal which added the wireless tag holding the user ID and the password which normal was allowed, it becomes impossible to access it to the resource of LANs 102A-102C, and it can prevent unlawful access to an inaccurate user. Moreover, since LAN configuration information is not disclosed at all by the inaccurate user, the safety of LANs 102A-102C can be raised.
[0023] Moreover, if it is the wireless LAN terminal which added the wireless tag holding the user ID and the password which normal was allowed even if the manager of LANs 102A-102C is absent, since LAN configuration information will be set as the LAN configuration information setting field 1403, without making a user conscious, temporary use is also attained even if it is a manager absence.
[0024] In addition, it may be made to carry out in the wireless LAN base station 101 instead of performing authentication processing by the authentication server 103. In that case, you may make it acquire the authentication information 502 from an authentication server 103 or other external devices, and it may be beforehand held in the wireless LAN base station 101.
[0025] Drawing 5 is the flow Fig. having shown the procedure of authentication of a wireless LAN terminal, and LAN connection. The wireless LAN base station 101 emits the signal which looks for the wireless LAN terminals 104A and 104B, and is supervising that the wireless LAN terminals 104A and 104B invaded within self-(step 501). If the wireless LAN terminal which invaded is undiscovered, it will scan continuously. When one of wireless LAN terminals is discovered (step 502), the wireless LAN base station 101 transmits the authentication information acquisition demand for attesting to the wireless LAN terminal (step 503). The wireless LAN terminal which received the authentication information acquisition demand returns the authentication information currently held in the wireless tag in the end of a local (step 504).
[0026] In order to use the returned authentication information for the wireless LAN base station 101 and to attest a wireless LAN terminal, the authentication processing demand which includes authentication information to an authentication server 103 is transmitted (step 505). An authentication server 103 performs authentication processing using the transmitted authentication information (step 506). This authentication processing is performed by collating with the authentication information 402 in an authentication server 103. When authentication is successful, the LAN configuration information for participating in LAN currently held in the authentication information 402 is returned to a wireless LAN terminal via the wireless LAN base station 101 (step 507,508).
[0027] At a wireless LAN terminal, when LAN configuration information is returned, LAN

configuration information is set up in a wireless LAN terminal (step 509), and it changes into the condition that a wireless LAN communication link can be performed. LAN configuration information is set up, and if it will be in the condition that connection with LANs 102A-102C can be made, data communication will be performed as a usual communication link (step 510). That is, a wireless LAN terminal sends out data by wireless to the wireless LAN base station 101. The wireless LAN base station 101 which received data chooses LANs 102A-102C connected to self-equipment based on received data (step 511), and transmits data to one of the selected LAN of the. Thereby, it enables a wireless LAN terminal to be only holding authentication information within the end of a local, and to perform connection authentication to LANs 102A-102C, LAN selection, and data communication.

[0028] In addition, when detecting whether the wireless LAN terminals 104A or 104B invaded into electric-wave attainment within the limits of the wireless LAN base station 101, it may be made to consider by having transmitted the question signal with the same frequency band as wireless LAN, and having answered the identifier of the wireless LAN terminal with which the identifier of a wireless tag or the wireless tag concerned was added as the response from the wireless tag as invasion detection. If it does in this way, it will become unnecessary to incorporate processing (processing of step 503,504) for that wireless tag 106A holding the authentication information to which connection with LANs 102A-102C is permitted may be added to the wireless LAN terminal which a user owns to only send and receive authentication information in a wireless LAN terminal.

[0029] Drawing 6 is drawing having shown the outline of the LAN selection performed in the wireless LAN base station 101. The wireless LAN base station 101 receives the data from the wireless LAN terminals 104A and 104B. Although the wireless LAN base station 101 is usually transmitting received data to the interface by the side of LAN connected to self-equipment and enables a wireless LAN communication link, it chooses and transmits a suitable thing from two or more LANs connected in this invention according to the protocol information in the received data. Received data 601 consist of the protocol section 602 for performing radio, and a protocol 603 on transmitted LAN as a protocol which controls a communication link. the judgment 604 of LAN transmitted using the LAN protocol 603 constituted by the high order at the same time the wireless LAN base station 101 performs radio with the wireless protocol 602 -- it carries out. Into the LAN protocol 603, since the transmitting agency address and the transmission place address are included, the transmission place address is extracted and LAN which consists of the same addresses out of LANs 102A-102C connected to self-equipment is chosen. When LAN which consists of the same addresses does not exist, since LAN of the destination is a relay point, it transmits by choosing suitable LAN based on the routing information set up in self-equipment.

[0030] Drawing 7 is the system configuration Fig. showing the operation gestalt which was made to attest by installing an authentication server 103 in a remote place. This operation gestalt is using a general-purpose interface gestalt and a protocol as a connection interface of a base transceiver station 101 and an authentication server 103, and can free the installation of an authentication server 103. Thereby, it becomes possible to carry out the centralized control of the authentication information on two or more LANs by one place.

[0031] With this operation gestalt, the cellular-phone terminal 204 was used and the authentication server 202 is connected. In case authentication is needed with connection of a wireless LAN terminal, a base transceiver station 101 opens connection, now the authentication server interface which is to self-equipment. That is, after establishing the channel between portable telephones 701 and 702 and establishing connection with an authentication server 103, it attests here.

[0032]

[Effect of the Invention] As explained above, according to this invention, it becomes possible to perform selection of wireless LAN, participation, and a communication link, without [without a user is conscious of LAN configuration only by holding the authentication information for attesting in a wireless LAN terminal and] threatening safeties, such as a resource in wireless LAN. Moreover, it becomes possible to connect a wireless LAN terminal unit to either of two or more wireless LAN alternatively by one wireless LAN base station.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention] This invention detects the wireless LAN terminal which invaded into electric-wave attainment within the limits of a base transceiver station, and relates to a wireless LAN terminal unit at the approach and wireless LAN base station equipment list which control said wireless LAN terminal possible [connection] to either of two or more wireless LAN which uses the same frequency band identically within the area.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art] The wireless LAN terminal which a wireless LAN base station exists on one network of a LAN (Local Area Network) protocol, and communicates with the same wireless LAN base station in a wireless LAN system can be connected only with the wireless LAN which the wireless LAN base station has connected. A wireless LAN base station is equipped with a wireless interface and every one LAN interface, and exchange of a wireless protocol and a LAN protocol is performed by passing both communication links transparent. For this reason, an interface is set to 1:1 and serves as connection with one LAN to one radio frequency band.
[0003] Moreover, when a wireless LAN terminal connects with wireless LAN through a wireless LAN base station, after configuration information, such as a network address of the wireless LAN (or it participates) to connect, comes to hand beforehand, processing set as the interior of the wireless LAN terminal itself is performed, and connection with a wireless LAN base station and connection with wireless LAN are made. Moreover, authentication processing which it permits using the resource on wireless LAN is performed between a wireless LAN terminal and the authentication equipment currently installed on wireless LAN, after connection with wireless LAN is made. Only authentication is performed, after this is performed on LAN protocols, such as TCP/IP, and is in the condition in which a fundamental communication link is possible.
[0004]
[Problem(s) to be Solved by the Invention] By the way, at office or works, two or more wireless LAN doubled not only with single wireless LAN but with the application is laid in many cases. According to the laid wireless LAN, it is necessary to install two or more wireless LAN base stations in such an environment. On the other hand, the user of the wireless LAN terminal to connect needs to receive in advance the LAN configuration information (a network address, subnet mask, etc.) doubled with the wireless LAN of a connection place, and needs to perform a setup on a terminal.
[0005] However, since it becomes possible to access the resource of the fixed range on wireless LAN, making the user of a wireless LAN terminal receive the configuration information of wireless LAN beforehand becomes the cause which causes unlawful access of a resource, and it has the problem on management of a resource, or a security management of not being desirable. Moreover, configuration information, such as a network address, is given according to the fixed Ruhr in many cases, disclosing the configuration information on wireless LAN shows that an analogy of other equipment configurations on wireless LAN is attained, and this also has the problem of not being desirable, in respect of a security management.
[0006] On the other hand, since configuration information cannot come to hand when a manager is absent if the user of a wireless LAN terminal who expects connection of wireless LAN temporarily has it, although the configuration information of wireless LAN is managed by the manager in many cases, there is a problem that use is impossible temporarily. Moreover, although attested in a connection phase by the remote access by LAN using public lines, such as a telephone, at wireless LAN, it is rare to perform authentication on the connection level which makes a communication link possible, configuration information is set up, and connection with wireless LAN is attained by making connection

with a wireless LAN base station in many cases. However, on wireless LAN, since the resource which can be accessed even if it does not attest also exists, by the authentication processing after connection, the problem of it becoming impossible to secure sufficient security is.
[0007] It is made in order that this invention may solve such a problem, and the 1st purpose is in providing with a wireless LAN terminal unit the participating control approach to LAN of the wireless LAN terminal which enables connection of a wireless LAN terminal, and a wireless LAN base station equipment list, without threatening safeties, such as a resource in wireless LAN. The 2nd purpose of this invention is to provide with a wireless LAN terminal unit the participating control approach to the wireless LAN of the wireless LAN terminal which enables connection of a wireless LAN terminal unit alternatively by one wireless LAN base station at either of two or more wireless LAN, and a wireless LAN base station equipment list.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] As explained above, according to this invention, it becomes possible to perform selection of wireless LAN, participation, and a communication link, without [without a user is conscious of LAN configuration only by holding the authentication information for attesting in a wireless LAN terminal and] threatening safeties, such as a resource in wireless LAN. Moreover, it becomes possible to connect a wireless LAN terminal unit to either of two or more wireless LAN alternatively by one wireless LAN base station.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the system configuration Fig. showing the operation gestalt of this invention.
[Drawing 2] It is drawing having shown the example of a configuration of a wireless LAN terminal.
[Drawing 3] It is drawing having shown the example of a configuration of a wireless LAN base station.
[Drawing 4] They are a wireless LAN terminal and the explanatory view of the authentication processing performed between authentication servers.
[Drawing 5] It is the flow Fig. showing the procedure of authentication of a wireless LAN terminal, and LAN connection processing.
[Drawing 6] It is the explanatory view showing the outline of the LAN selection performed in a wireless LAN base station.
[Drawing 7] It is drawing showing the operation gestalt in the case of attesting by installing an authentication server in a remote place.
[Description of Notations]
101 [-- A wireless tag, 401 / -- Authentication information, 402 / -- Authentication information, 1013 / -- An authentication controlling mechanism, 1012 / -- A LAN communication link exchange style, 1042 / -- A processing unit, 1043 / -- A LAN configuration information setting field, 4022 / -- LAN configuration information.] -- A wireless LAN base station, 102A - 102 C--LAN, 103 -- An authentication server, 104A, 104B -- A wireless LAN terminal, 106A, 106B

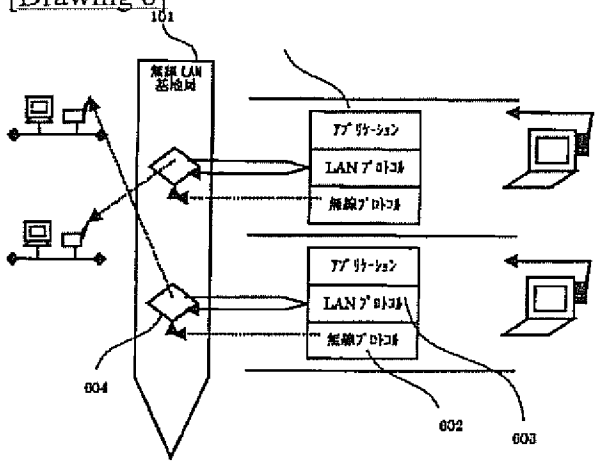
[Translation done.]

* NOTICES *

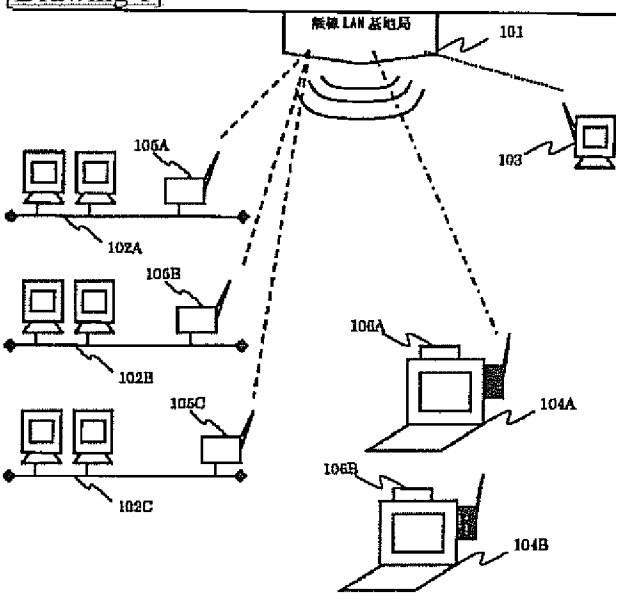
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

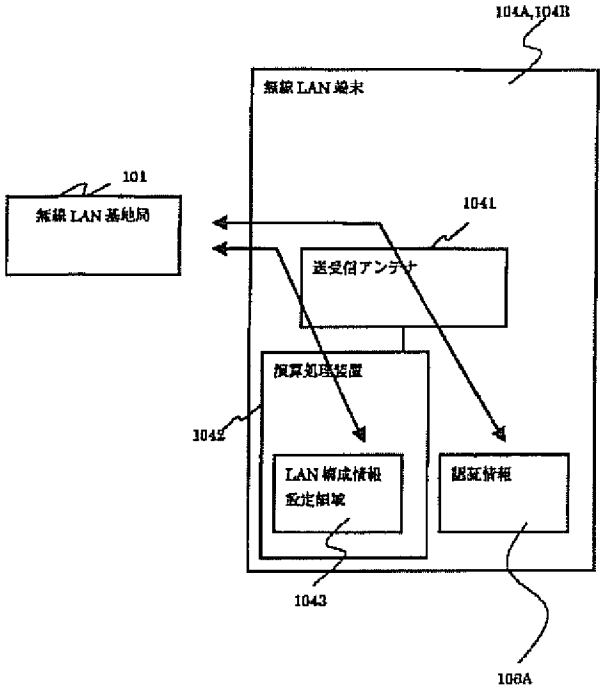
[Drawing 6]



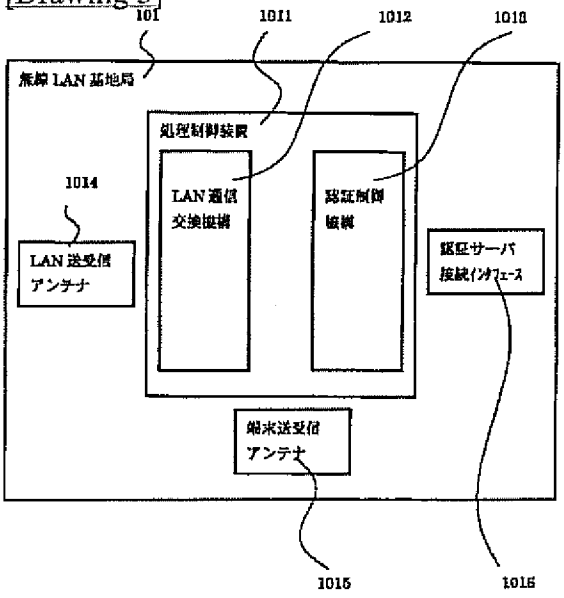
[Drawing 1]



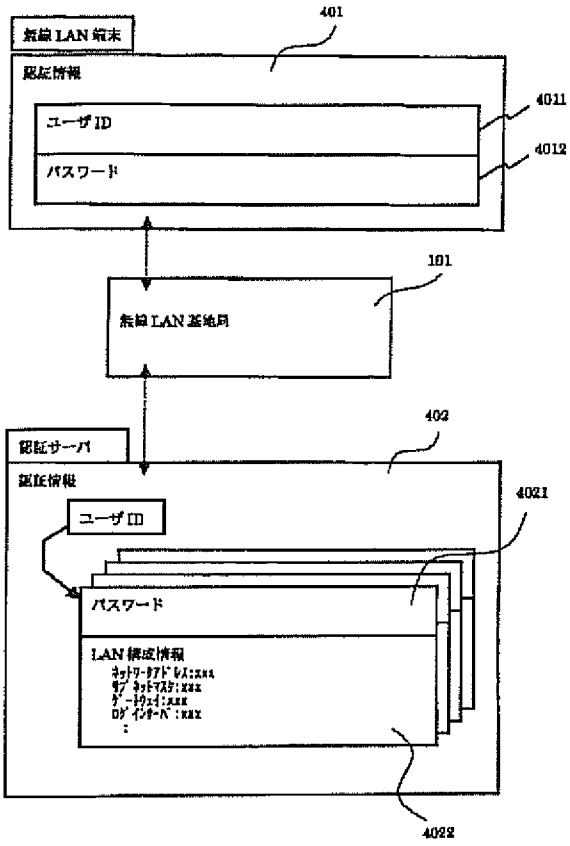
[Drawing 2]



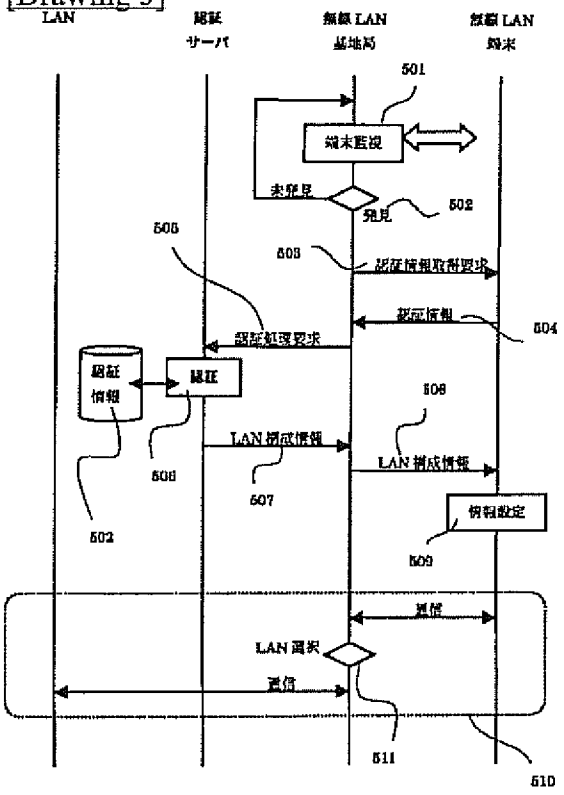
[Drawing 3]



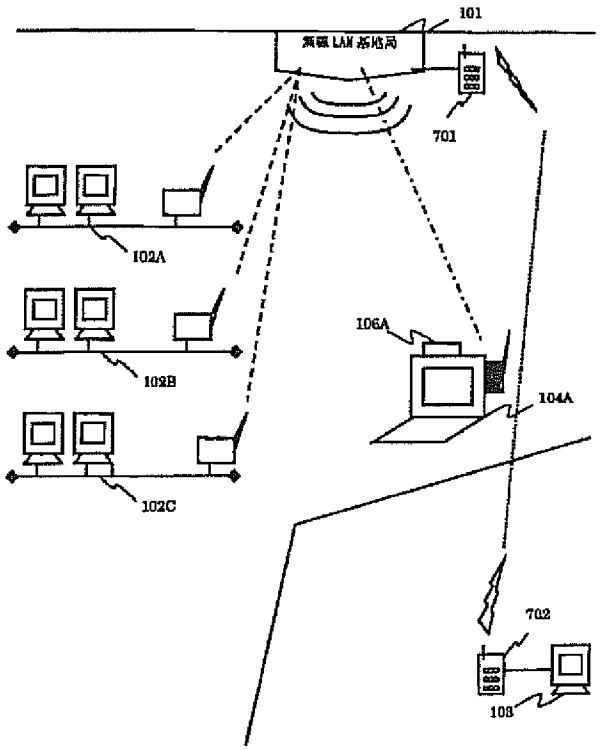
[Drawing 4]



[Drawing 5]



[Drawing 7]



[Translation done.]

HH/ETI/P0407

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－101545
(P2003－101545A)
(43)公開日　平成15年４月４日(2003.4.4)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/28	３００	Ｈ０４Ｌ　12/28	３００Ａ　５Ｋ０３３ ３００Ｍ

審査請求　未請求　請求項の数４　ＯＬ　（全８頁）

(21)出願番号　特願2001－285854(P2001－285854)

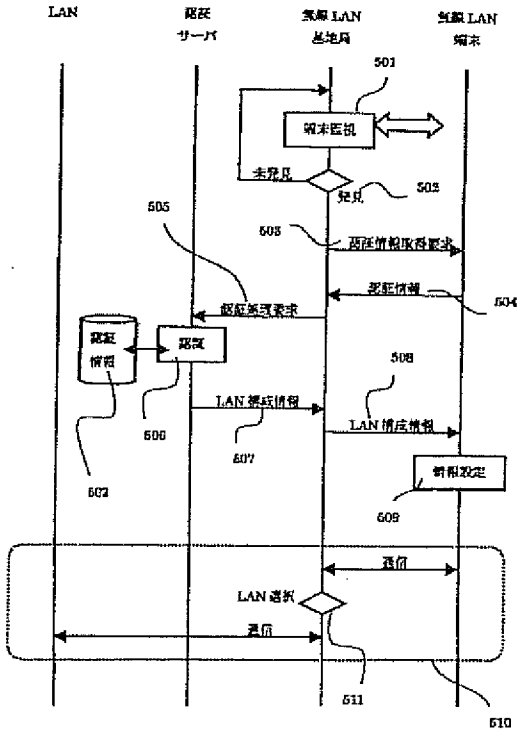
(22)出願日　平成13年９月19日(2001.9.19)

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市鶴見区末広町一丁目１番43
(72)発明者　池谷　誠一郎
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウエアエンジニアリング株式会社内
(74)代理人　100088720
弁理士　小川　眞一

最終頁に続く

(54)【発明の名称】　無線ＬＡＮ端末の無線ＬＡＮへの参加制御方法および無線ＬＡＮ基地局装置並びに無線ＬＡＮ端末装置

(57)【要約】
【課題】　無線ＬＡＮ内のリソースなどの安全性を脅かすことなく、無線ＬＡＮ端末の接続を可能にする無線ＬＡＮ端末のＬＡＮへの参加制御方法および無線ＬＡＮ基地局装置並びに無線ＬＡＮ端末装置を提供すること。
【解決手段】　無線基地局において自装置の電波到達範囲内に侵入した無線ＬＡＮ端末を検知し、当該無線ＬＡＮ端末に付加された無線タグから認証情報を取得するステップと、無線基地局内に設定された認証情報または無線基地局と接続された認証装置から取得した認証情報と前記無線タグから取得した認証情報とを照合し、複数の無線ＬＡＮのいずれかへの接続を許可するか否かを判定するステップと、接続許可の判定結果をもとに、無線基地局内に設定された複数の無線ＬＡＮの構成情報または無線基地局と接続された外部装置から取得した複数の無線ＬＡＮの構成情報を前記無線ＬＡＮ端末に送信するステップとを備える。



1

【特許請求の範囲】

【請求項１】　無線基地局の電波到達範囲内に侵入した無線ＬＡＮ端末を検知し、同一域内で同一の周波数帯を使用する複数の無線ＬＡＮのいずれかに対し前記無線ＬＡＮ端末を接続可能に制御する方法であって、

前記無線基地局において自装置の電波到達範囲内に侵入した無線ＬＡＮ端末を検知し、当該無線ＬＡＮ端末に付加された無線部品から認証情報を取得するステップと、

無線基地局内に設定された認証情報または無線基地局と接続された認証装置から取得した認証情報と前記無線部品から取得した認証情報とを照合し、複数の無線ＬＡＮのいずれかへの接続を許可するか否かを判定するステップと、

接続許可の判定結果をもとに、無線基地局内に設定された複数の無線ＬＡＮの構成情報または無線基地局と接続された外部装置から取得した複数の無線ＬＡＮの構成情報を前記無線ＬＡＮ端末に送信するステップと、

無線ＬＡＮ端末において前記無線基地局から受信した前記無線ＬＡＮ構成情報を自端末内に設定し、当該無線ＬＡＮ構成情報に従って複数の無線ＬＡＮのいずれかに接続可能にするステップとを備えることを特徴とする無線ＬＡＮ端末の無線ＬＡＮへの参加制御方法。

【請求項２】　自装置の電波到達範囲内に侵入した無線ＬＡＮ端末を検知し、同一域内で同一の周波数帯を使用する複数の無線ＬＡＮのいずれかに対し前記無線ＬＡＮ端末を接続可能に制御する装置であって、

自装置の電波到達範囲内に侵入した無線ＬＡＮ端末を検知し、当該無線ＬＡＮ端末に付加された無線部品から認証情報を取得する手段と、

自装置内に設定された認証情報または自装置と接続された認証装置から取得した認証情報と前記無線部品から取得した認証情報とを照合し、複数の無線ＬＡＮのいずれかへの接続を許可するか否かを判定する手段と、

接続許可の判定結果をもとに、自装置内に設定された複数の無線ＬＡＮの構成情報または自装置と接続された外部装置から取得した複数の無線ＬＡＮの構成情報を前記無線ＬＡＮ端末に送信し、設定する手段とを備えることを特徴とする無線ＬＡＮ基地局装置。

【請求項３】　無線ＬＡＮ端末との無線通信プロトコルの上位のプロトコルに基づいて無線ＬＡＮ端末から複数の無線ＬＡＮへの通信を振り分ける手段を備えることを特徴とする請求項２に記載の無線ＬＡＮ基地局装置。

【請求項４】　無線基地局からの制御に基づき、同一域内で同一の周波数帯を使用する複数の無線ＬＡＮのいずれかに対し接続可能状態に制御される無線ＬＡＮ端末装置であって、

前記無線基地局からの要求に従い自装置の認証情報を無線によって返信する無線部品と、

前記無線基地局における認証処理に応じて前記無線基地局から送信される無線ＬＡＮ構成情報を受信し、自装置内に設定し、当該無線ＬＡＮ構成情報に従って複数の無線ＬＡＮのいずれかに接続可能にする手段とを備えることを特徴とする無線ＬＡＮ端末装置。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、無線基地局の電波到達範囲内に侵入した無線ＬＡＮ端末を検知し、同一域内で同一の周波数帯を使用する複数の無線ＬＡＮのいずれかに対し前記無線ＬＡＮ端末を接続可能に制御する方法および無線ＬＡＮ基地局装置並びに無線ＬＡＮ端末装置に関するものである。

【０００２】

【従来の技術】無線ＬＡＮシステムでは、ＬＡＮ（Local Area Network）プロトコルの１つのネットワーク上に無線ＬＡＮ基地局が存在し、同一の無線ＬＡＮ基地局と通信を行なう無線ＬＡＮ端末は、無線ＬＡＮ基地局が接続している無線ＬＡＮにのみ接続を行なうことが可能である。無線ＬＡＮ基地局は、無線インタフェースとＬＡＮインタフェースを１つずつ備え、双方の通信を透過的に通過させることで無線プロトコル、ＬＡＮプロトコルの交換を行なう。このため、インタフェースは１：１となり、１つの無線周波数帯に対して、１つのＬＡＮとの接続となっている。

【０００３】また、無線ＬＡＮ端末が無線ＬＡＮ基地局を介して無線ＬＡＮに接続を行なう際には、接続する（あるいは参加する）無線ＬＡＮのネットワークアドレス等の構成情報を予め入手した上で、無線ＬＡＮ端末自身の内部に設定する処理を行い、無線ＬＡＮ基地局との接続、無線ＬＡＮとの接続を行なう。また、無線ＬＡＮ上のリソースを使用することを許可する認証処理は、無線ＬＡＮへの接続が行われた後、無線ＬＡＮ端末と無線ＬＡＮ上に設置されている認証装置との間で行われる。これは、TCP/IPなどのＬＡＮプロトコルの上で行われるもので、基本的な通信が可能な状態になってから認証のみが行われる。

【０００４】

【発明が解決しようとする問題】ところで、オフィスや工場などでは、単一の無線ＬＡＮのみでなく、用途に合わせた複数の無線ＬＡＮが敷設されていることも多い。このような環境においては、敷設された無線ＬＡＮに合わせて、複数の無線ＬＡＮ基地局を設置する必要がある。一方、接続する無線ＬＡＮ端末の利用者は、接続先の無線ＬＡＮに合わせたＬＡＮ構成情報(ネットワークアドレス、サブネットマスクなど)を事前入手し、端末上の設定を行なう必要がある。

【０００５】しかし、無線ＬＡＮの構成情報を予め無線ＬＡＮ端末の利用者に入手させるということは、無線ＬＡＮ上の一定の範囲のリソースにアクセスすることが可能となるため、リソースの不正アクセスを招く原因となり、リソースの管理やセキュリティ管理の上での好まし

くないという問題がある。また、ネットワークアドレスなどの構成情報は、一定のルールに従って付与されることが多く、無線ＬＡＮ上の構成情報を開示するということは、無線ＬＡＮ上の他の装置構成が類推可能になることを示し、これもまたセキュリティ管理という点で好ましくないという問題がある。

【０００６】一方、無線ＬＡＮの構成情報は、管理者により管理されていることが多いが、一時的に無線ＬＡＮに接続を希望する無線ＬＡＮ端末の利用者にあっては、管理者が不在であった場合には構成情報を入手できないために、一時利用ができないという問題がある。また、電話などの公衆回線を用いＬＡＮへのリモートアクセスでは、接続段階で認証を行なうが、無線ＬＡＮでは、通信を可能にする接続レベルでの認証を行なうことは少なく、構成情報を設定し、無線ＬＡＮ基地局との接続を行なうことで無線ＬＡＮへの接続が可能になることが多い。しかし、無線ＬＡＮ上には、認証を行なわなくてもアクセスすることが可能なリソースも存在するため、接続後の認証処理では、十分なセキュリティが確保できなくなるという問題がある。

【０００７】本発明は、このような問題を解決するためになされたものであり、その第１の目的は、無線ＬＡＮ内のリソースなどの安全性を脅かすことなく、無線ＬＡＮ端末の接続を可能にする無線ＬＡＮ端末のＬＡＮへの参加制御方法および無線ＬＡＮ基地局装置並びに無線ＬＡＮ端末装置を提供することにある。本発明の第２の目的は、１つの無線ＬＡＮ基地局により複数の無線ＬＡＮのいずれかに無線ＬＡＮ端末装置を選択的に接続可能にする無線ＬＡＮ端末の無線ＬＡＮへの参加制御方法および無線ＬＡＮ基地局装置並びに無線ＬＡＮ端末装置を提供することにある。

【０００８】

【課題を解決するための手段】上記目的を達成するために、本発明の無線ＬＡＮ端末の無線ＬＡＮへの参加制御方法は、無線基地局の電波到達範囲内に侵入した無線ＬＡＮ端末を検知し、同一域内で同一の周波数帯を使用する複数の無線ＬＡＮのいずれかに対し前記無線ＬＡＮ端末を接続可能に制御する方法であって、前記無線基地局において自装置の電波到達範囲内に侵入した無線ＬＡＮ端末を検知し、当該無線ＬＡＮ端末に付加された無線部品から認証情報を取得するステップと、無線基地局内に設定された認証情報または無線基地局と接続された認証装置から取得した認証情報と前記無線部品から取得した認証情報とを照合し、複数の無線ＬＡＮのいずれかへの接続を許可するか否かを判定するステップと、接続許可の判定結果をもとに、無線基地局内に設定された複数の無線ＬＡＮの構成情報または無線基地局と接続された外部装置から取得した複数の無線ＬＡＮの構成情報を前記無線ＬＡＮ端末に送信するステップと、無線ＬＡＮ端末において前記無線基地局から受信した前記無線ＬＡＮ構成情報を自端末内に設定し、当該無線ＬＡＮ構成情報に従って複数の無線ＬＡＮのいずれかに接続可能にするステップとを備えることを特徴とする。

【０００９】本発明の無線ＬＡＮ基地局装置は、自装置の電波到達範囲内に侵入した無線ＬＡＮ端末を検知し、同一域内で同一の周波数帯を使用する複数の無線ＬＡＮのいずれかに対し前記無線ＬＡＮ端末を接続可能に制御する装置であって、自装置の電波到達範囲内に侵入した無線ＬＡＮ端末を検知し、当該無線ＬＡＮ端末に付加された無線部品から認証情報を取得する手段と、自装置内に設定された認証情報または自装置と接続された認証装置から取得した認証情報と前記無線部品から取得した認証情報とを照合し、複数の無線ＬＡＮのいずれかへの接続を許可するか否かを判定する手段と、接続許可の判定結果をもとに、自装置内に設定された複数の無線ＬＡＮの構成情報または自装置と接続された外部装置から取得した複数の無線ＬＡＮの構成情報を前記無線ＬＡＮ端末に送信し、設定する手段とを備えることを特徴とする。また、無線ＬＡＮ端末との無線通信プロトコルの上位のプロトコルに基づいて無線ＬＡＮ端末から複数の無線ＬＡＮへの通信を振り分ける手段を備えることを特徴とする。

【００１０】また、本発明に係る無線ＬＡＮ端末装置は、無線基地局からの制御に基づき、同一域内で同一の周波数帯を使用する複数の無線ＬＡＮのいずれかに対し接続可能状態に制御される無線ＬＡＮ端末装置であって、前記無線基地局からの要求に従い自装置の認証情報を無線によって返信する無線部品と、前記無線基地局における認証処理に応じて前記無線基地局から送信される無線ＬＡＮ構成情報を受信し、自装置内に設定し、当該無線ＬＡＮ構成情報に従って複数の無線ＬＡＮのいずれかに接続可能にする手段とを備えることを特徴とする。

【００１１】

【発明の実施の形態】以下、本発明を実施する場合の一形態を図面に基づいて具体的に説明する。図１は、本発明の実施形態を示すシステム構成図である。本発明は、アンテナを内蔵または外部接続した無線ＬＡＮの基地局１０１と、この１つの無線ＬＡＮ基地局１０１に収容された複数のＬＡＮ１０２Ａ～１０２Ｃと、これらのＬＡＮ１０２Ａ～１０２Ｃへの参加を許すか否かを認証するための認証サーバ１０３と、ＬＡＮ１０２Ａ～１０２Ｃへの接続を制御する無線ＬＡＮ基地局１０１と通信を可能とする複数の無線ＬＡＮ端末１０４Ａ，１０４Ｂから構成される。複数のＬＡＮ１０２Ａ～１０２Ｃは、無線ＬＡＮ基地局１０１との間で無線回線により通信を行なう送受信装置１０５Ａ～１０５Ｃが接続されている。この送受信装置１０５Ａ～１０５Ｃが接続されたことにより、ＬＡＮ１０２Ａ～１０２Ｃは同一域内で同一の周波数帯を使用する無線ＬＡＮとしての機能が付加される。

【００１２】一方、無線ＬＡＮ基地局１０１は、自局１

０１の電波到達範囲内に侵入した無線ＬＡＮ端末１０４Ａ，１０４Ｂを検知し、その検知した無線ＬＡＮ端末１０４Ａ１０４Ｂから認証情報を無線回線で取得し、その取得した認証情報を認証サーバ１０２に無線または有線回線で転送し、ＬＡＮ１０２Ａ～１０２Ｃへの接続を許可するか否かの認証処理を実行させ、認証ＯＫの応答が得られたならば、ＬＡＮ１０２Ａ～１０２Ｃの構成情報をＬＡＮ端末１０４Ａ，１０４Ｂに送信する。ＬＡＮ１０２Ａ～１０２Ｃの構成情報を受信したＬＡＮ端末１０４Ａ，１０４Ｂでは、その構成情報を自装置内のメモリ内に登録し、その登録内容を参照してＬＡＮ１０２Ａ～１０２Ｃのいずれかに接続要求を発し、通信を行なう。

【００１３】無線ＬＡＮ端末１０４Ａ，１０４Ｂには、ＬＡＮ１０２Ａ～１０２Ｃに接続するための認証情報が登録された無線タグ（無線部品）１０６Ａ，１０６Ｂが筐体の一部に付加されている。この無線タグ１０６Ａ，１０６Ｂに登録された認証情報は、無線ＬＡＮ基地局１０１からの問い合わせ信号に応答して無線ＬＡＮ基地局１０１へ返信される。この無線タグ１０６Ａ，１０６Ｂは、無指向性のアンテナと電池、ＬＳＩメモリを内蔵しており、無線ＬＡＮ基地局１０１からの問い合わせ信号に応じて、登録されている認証情報を応答信号として返信する。

【００１４】図２は、無線ＬＡＮ端末１０４Ａの詳細構成例を示した図である。無線ＬＡＮ端末１０４Ａは、無線ＬＡＮ基地局１０１との通信を行なうための送受信アンテナ１０４１と通信したデータの処理、分析を行なう演算処理装置１０４２とから構成され、筐体の一部に無線タグ１０６Ａが取り付けられている。演算処理装置１０４２には、無線ＬＡＮ基地局１０１１より送信されてくるＬＡＮ１０２Ａ～１０２Ｃに接続するための構成情報を保持するためのＬＡＮ構成情報設定領域１０４３がメモリ内に確保されている。このＬＡＮ構成情報設定領域１０４３に設定される情報は、無線接続を行なう構成情報のほかに、ＬＡＮ１０２Ａ～１０２Ｃとの接続を可能とする構成情報を保持する。一般的には、TCP/IPが使用され、IPアドレス、ネットワークアドレス、ゲートウェイアドレス、各種サーバアドレス等の情報がＬＡＮ構成情報の内容である。

【００１５】一方、無線タグ１０６Ａに登録される認証情報は、ＬＡＮ１０２Ａ～１０２Ｃに参加をするための認証情報であり、最低限、自装置１０４Ａを特定するためのユニークな識別子とパスワードより構成される。図３は、無線ＬＡＮ基地局１０１の詳細構成例を示した図である。無線ＬＡＮ基地局１０１は、従来における基地局の持つ機能である無線ＬＡＮ端末とＬＡＮ間の無線通信のみでなく、無線ＬＡＮ端末の侵入監視、接続前認証処理、ＬＡＮ間通信の交換の機能を持つ。

【００１６】この例の無線ＬＡＮ基地局１０１は、通信、認証などの機能の中心となる処理制御装置１０１１を有し、処理制御装置１０１１には、無線通信の制御を行なうＬＡＮ通信交換機構１０１２、認証の制御を行なう認証制御機構１０１３より構成される。処理制御装置１０１１には、通信対象となるＬＡＮ１０２Ａ～１０２Ｃの送受信装置１０５Ａ～１０５Ｃと通信を行なうＬＡＮ送受信アンテナ１０１４、無線ＬＡＮ端末１０４Ａ，１０４Ｂとの通信を行なう端末送受信アンテナ１０１５を有する。また、無線ＬＡＮ基地局１０１は、認証サーバ１０３と接続するための認証サーバ接続インタフェース１０１６を有する。

【００１７】無線ＬＡＮ基地局１０１は、端末送受信アンテナ１０１５から端末検知のための電波を所定時間間隔で送出し、いずれかの無線ＬＡＮ端末が自局の電波到達範囲内に侵入したかどうかを監視しており、侵入した検知した場合には、その検知した無線ＬＡＮ端末の無線タグ１０６Ａまたは１０６Ｂから認証情報を取得し、その取得した認証情報を認証制御機構１０１３の処理によって認証サーバ１０３に転送し、認証処理を実行させる。認証ＯＫの応答が認証サーバ１０３から返信されたならば、ＬＡＮ１０２Ａ１０２Ｃのネットワークアドレスなどの構成情報を認証サーバ１０３から取得し、侵入を検知した無線ＬＡＮ端末に送信し、その無線ＬＡＮ端末のＬＡＮ構成情報設定領域１４０３の設定させる。

【００１８】これにより、無線ＬＡＮ基地局１０１の電波到達範囲内に侵入した無線ＬＡＮ端末１０４Ａまたは１０４Ｂは無線ＬＡＮ基地局１０１を通じて１０２Ａ～１０２Ｃのいずれかに接続可能になる。この場合、接続対象となるＬＡＮ１０２Ａ～１０２Ｃは、TCP/IPなどの上位プロトコル情報をＬＡＮ通信交換機構１０１２で解析し、その解析結果に従って選択される。このような１つの無線ＬＡＮ基地局１０１における複数のＬＡＮへの接続振り分け処理によって、全体としては、１つの無線ＬＡＮ基地局内に複数のＬＡＮを多重化して収容した無線ＬＡＮシステムが構築されたことになる。

【００１９】図４は、無線ＬＡＮ端末１０４Ａ，１０４Ｂと認証サーバ１０３間で行われるＬＡＮ接続認証処理の説明図である。無線ＬＡＮ基地局１０１は、自局の電波影響範囲内への無線ＬＡＮ端末１０４Ａ，１０４Ｂの侵入を常時監視しているが、侵入が検知されると、無線ＬＡＮ基地局１０１、無線ＬＡＮ端末１０４Ａ，１０４Ｂ、認証サーバ１０３の間で認証処理を実行する。無線ＬＡＮ端末１０４Ａ，１０４Ｂには、少なくともユーザＩＤ４０１１、パスワード４０１２から成る認証情報４０１を保持した無線タグ１０６Ａ、１０６Ｂが付加されている。ユーザＩＤ４０１１は、無線ＬＡＮ端末１０４Ａ，１０４Ｂをユニークに特定するための情報であり、認証サーバ１０３上のデータを検索するためのキー情報となる。パスワード４０１２は、認証サーバ１０３上のパスワードと照合され、無線ＬＡＮ端末１０４Ａ，１０４Ｂ上の認証情報が正規に登録されたものか（正規にＬ

ＡＮへの接続を許可されたものか）を識別するための情報として使用される。

【００２０】認証サーバ１０３には、パスワード４０２１と接続をＬＡＮ１０２Ａ～１０２Ｃへの接続を許可するＬＡＮ構成情報４０２２をユーザＩＤをキーとして検索できるように保持されている。無線ＬＡＮ基地局１０１は、侵入を検知した無線ＬＡＮ端末１０４Ａまたは１０４Ｂから取得した認証情報４０１のユーザＩＤ４０１１、パスワード４０１２を認証サーバ１０３に送信する。認証サーバ１０３では、受信したユーザＩＤ４０１１をキーとして、内部に保持されている認証情報４０２を検索する。対応する認証情報が保持されている場合は、パスワード４０１２の照合を行い、一致することを確認する。一致した場合、認証成功とし、ユーザＩＤ４０１１で検索されるＬＡＮ構成情報４０２２を認証結果として無線ＬＡＮ基地局１０１に返信する。

【００２１】無線ＬＡＮ基地局１０１は、返信されたＬＡＮ構成情報４０２２を侵入検知した無線ＬＡＮ端末１０４Ａまたは１０４Ｂに送信する。これに対し、無線ＬＡＮ端末１０４Ａまたは１０４Ｂでは、受信したＬＡＮ構成情報４０２２をＬＡＮ構成情報設定領域１４０３に登録する。これにより、ＬＡＮ構成情報４０２２を用いて、ＬＡＮ１０２Ａ～１０２５Ｃへの参加が可能となる。この場合、ユーザＩＤ毎に、ＬＡＮ構成情報４０２２の内容を異なるように設定できるので、ユーザによってＬＡＮ１０２Ａ～１０２Ｃのいずれに接続可能であるかを制御することができる。

【００２２】なお、認証失敗となった場合には、該当する無線ＬＡＮ端末にはエラー応答が送信され、ＬＡＮ構成情報は送信されない。従って、ＬＡＮ１０２Ａ～１２Ｃへの参加は不可能になり、正規に許されたユーザＩＤおよびパスワードを保持した無線タグを付加した無線ＬＡＮ端末以外はＬＡＮ１０２Ａ～１０２Ｃのリソースへアクセスすることができなくなり、不正利用者に不正アクセスを防止することができる。また、ＬＡＮ構成情報が不正利用者に全く開示されないので、ＬＡＮ１０２Ａ～１０２Ｃの安全性を高めることができる。

【００２３】また、ＬＡＮ１０２Ａ～１０２Ｃの管理者が不在であっても、正規に許されたユーザＩＤおよびパスワードを保持した無線タグを付加した無線ＬＡＮ端末であれば、ユーザに意識させることなく、ＬＡＮ構成情報がＬＡＮ構成情報設定領域１４０３に設定されるので、管理者不在であっても一時的利用も可能になる。

【００２４】なお、認証処理は認証サーバ１０３で行なう代わりに、無線ＬＡＮ基地局１０１で行なうようにしても良い。その場合、認証情報５０２は、認証サーバ１０３または他の外部装置から取得するようにしてもよいし、無線ＬＡＮ基地局１０１内に予め保持しておくようにしても良い。

【００２５】図５は、無線ＬＡＮ端末の認証、ＬＡＮ接続の手順を示したフロー図である。無線ＬＡＮ基地局１０１は、無線ＬＡＮ端末１０４Ａ，１０４Ｂを探索する信号を発し、自域内に無線ＬＡＮ端末１０４Ａ、１０４Ｂが侵入したことを監視している（ステップ５０１）。侵入した無線ＬＡＮ端末が未発見であれば、継続して走査を行なう。いずれかの無線ＬＡＮ端末を発見した場合（ステップ５０２）、無線ＬＡＮ基地局１０１は、その無線ＬＡＮ端末に対して認証を行なうための認証情報取得要求を送信する（ステップ５０３）。認証情報取得要求を受信した無線ＬＡＮ端末は、自端末の無線タグ内に保持している認証情報を返送する（ステップ５０４）。

【００２６】無線ＬＡＮ基地局１０１は、返送された認証情報を使用し、無線ＬＡＮ端末の認証を行なうために、認証サーバ１０３に対して認証情報を含む認証処理要求を送信する（ステップ５０５）。認証サーバ１０３は、送信されてきた認証情報を用いて、認証処理を行なう（ステップ５０６）。この認証処理は、認証サーバ１０３内の認証情報４０２と照合することにより行われる。認証が成功した場合は、認証情報４０２内に保持されているＬＡＮに参加するためのＬＡＮ構成情報が無線ＬＡＮ基地局１０１を経由し、無線ＬＡＮ端末に返送される（ステップ５０７，５０８）。

【００２７】無線ＬＡＮ端末では、ＬＡＮ構成情報が返送された場合、無線ＬＡＮ端末内にＬＡＮ構成情報を設定し（ステップ５０９）、無線ＬＡＮ通信が行なえる状態にする。ＬＡＮ構成情報を設定し、ＬＡＮ１０２Ａ～１０２Ｃとの接続が行なえる状態になれば、通常の通信としてデータ通信を行なう（ステップ５１０）。すなわち、無線ＬＡＮ端末は、無線ＬＡＮ基地局１０１に対して無線によりデータを送出する。データを受信した無線ＬＡＮ基地局１０１は受信データに基づき、自装置に接続されているＬＡＮ１０２Ａ～１０２Ｃの選択を行い（ステップ５１１）、その選択したＬＡＮの１つにデータを転送する。これにより、無線ＬＡＮ端末は、自端末内に認証情報を保持するのみで、ＬＡＮ１０２Ａ～１０２Ｃへの接続認証、ＬＡＮ選択、データ通信を行なうことが可能になる。

【００２８】なお、無線ＬＡＮ端末１０４Ａまたは１０４Ｂが無線ＬＡＮ基地局１０１の電波到達範囲内に侵入したかを検知する場合、質問信号を無線ＬＡＮと同一周波数帯で送信し、その応答として無線タグの識別子または当該無線タグが付加された無線ＬＡＮ端末の識別子が無線タグから返信されたことによって、侵入検知とするようにしてもよい。このようにすれば、ＬＡＮ１０２Ａ～１０２Ｃへの接続を許可する認証情報を保持した無線タグ１０６Ａを、ユーザが所有する無線ＬＡＮ端末に付加しておくのみでよく、無線ＬＡＮ端末内に認証情報を送受するための処理（ステップ５０３，５０４の処理）を組み込んでおく必要がなくなる。

【００２９】図６は、無線ＬＡＮ基地局１０１内で行わ

れるＬＡＮ選択の概要を示した図である。無線ＬＡＮ基地局１０１は、無線ＬＡＮ端末１０４Ａ，１０４Ｂからのデータを受信する。無線ＬＡＮ基地局１０１は、通常は、自装置に接続されているＬＡＮ側のインタフェースに受信データを転送することで、無線ＬＡＮ通信を可能にするが、本発明においては、受信したデータ内のプロトコル情報に応じて、接続されている複数のＬＡＮから適切なものを選択して、転送する。受信データ６０１は、通信を制御するプロトコルとして、無線通信を行なうためのプロトコル部６０２、転送されたＬＡＮ上のプロトコル６０３で構成される。無線ＬＡＮ基地局１０１は、無線プロトコル６０２で無線通信を行なうと同時に、その上位に構成されるＬＡＮプロトコル６０３を用いて、転送するＬＡＮの判定６０４行なう。ＬＡＮプロトコル６０３中には、送信元アドレス、送信先アドレスが含まれるため、送信先アドレスを抽出し、自装置に接続されるＬＡＮ１０２Ａ～１０２Ｃの中から同一のアドレスで構成されるＬＡＮを選択する。同一アドレスで構成されるＬＡＮが存在しない場合、転送先のＬＡＮは中継点であるため、自装置内に設定されるルーティング情報に基づいて、適切なＬＡＮを選択して転送を行なう。

【００３０】図７は、認証サーバ１０３を遠隔地に設置し、認証を行なうようにした実施形態を示すシステム構成図である。この実施形態は、無線基地局１０１と認証サーバ１０３の接続インタフェースとして、汎用的なインタフェース形態、プロトコルを使用することで、認証サーバ１０３の設置場所を自由にすることが可能である。これにより、複数のＬＡＮの認証情報を一箇所で集中管理することが可能になる。

【００３１】この実施形態では、携帯電話端末２０４を使用し、認証サーバ２０２を接続している。無線ＬＡＮ端末の接続により認証が必要になった際、無線基地局１０１は自装置に接続さている認証サーバインタフェース＊＊を開く。すなわち、ここでは、携帯電話機７０１と７０２の間の通信路を確立し、認証サーバ１０３との接続を確立した上で、認証を行なう。

【００３２】

【発明の効果】以上に説明したように、本発明によれば、無線ＬＡＮ端末中に認証を行なうための認証情報を保持するだけで、使用者がＬＡＮ構成を意識することなく、また無線ＬＡＮ内のリソースなどの安全性を脅かすことなく、無線ＬＡＮの選択、参加、通信を行なうことが可能になる。また、１つの無線ＬＡＮ基地局により複数の無線ＬＡＮのいずれかに無線ＬＡＮ端末装置を選択的に接続することが可能になる。

【図面の簡単な説明】

【図１】本発明の実施形態を示すシステム構成図である。

【図２】無線ＬＡＮ端末の構成例を示した図である。

【図３】無線ＬＡＮ基地局の構成例を示した図である。

【図４】無線ＬＡＮ端末と認証サーバ間で行われる認証処理の説明図である。

【図５】無線ＬＡＮ端末の認証、ＬＡＮ接続処理の手順を示すフロー図である。

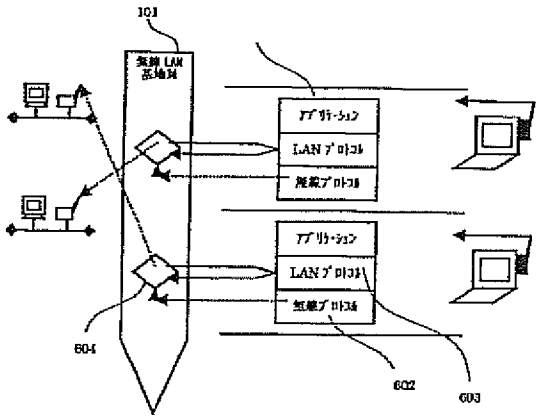
【図６】無線ＬＡＮ基地局内で行われるＬＡＮ選択の概要を示す説明図である。

【図７】認証サーバを遠隔地に設置し、認証を行なう場合の実施形態を示す図である。

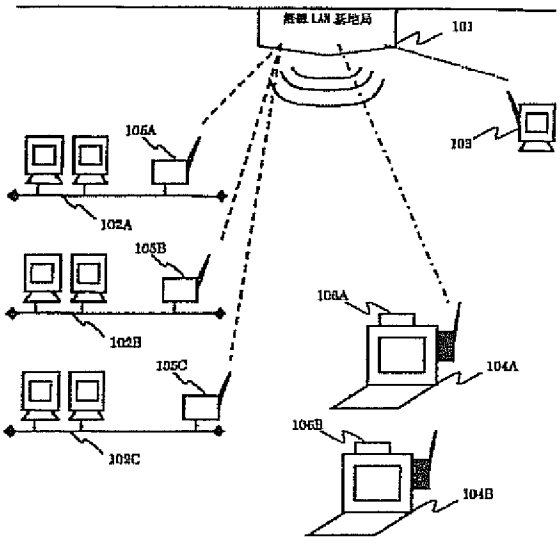
【符号の説明】

１０１…無線ＬＡＮ基地局、１０２Ａ～１０２Ｃ…ＬＡＮ、１０３…認証サーバ、１０４Ａ，１０４Ｂ…無線ＬＡＮ端末、１０６Ａ、１０６Ｂ…無線タグ、４０１…認証情報、４０２…認証情報、１０１３…認証制御機構、１０１２…ＬＡＮ通信交換機構、１０４２…演算処理装置、１０４３…ＬＡＮ構成情報設定領域、４０２２…ＬＡＮ構成情報。

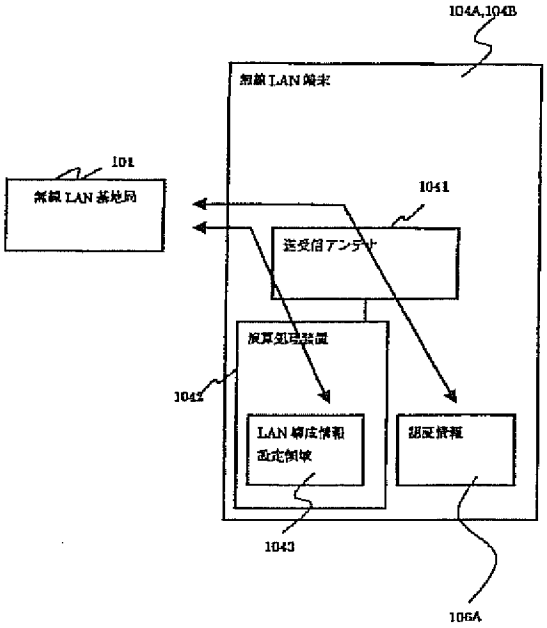
【図６】



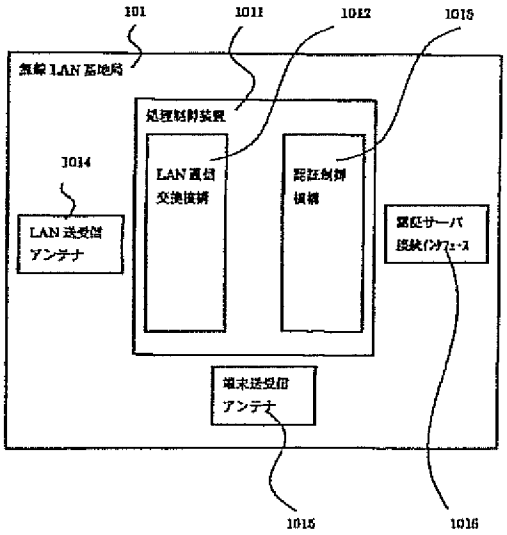
【図1】


無線 LAN 基地局
101
105A
102A
103
105B
102B
106A
104A
105C
102C
106B
104B

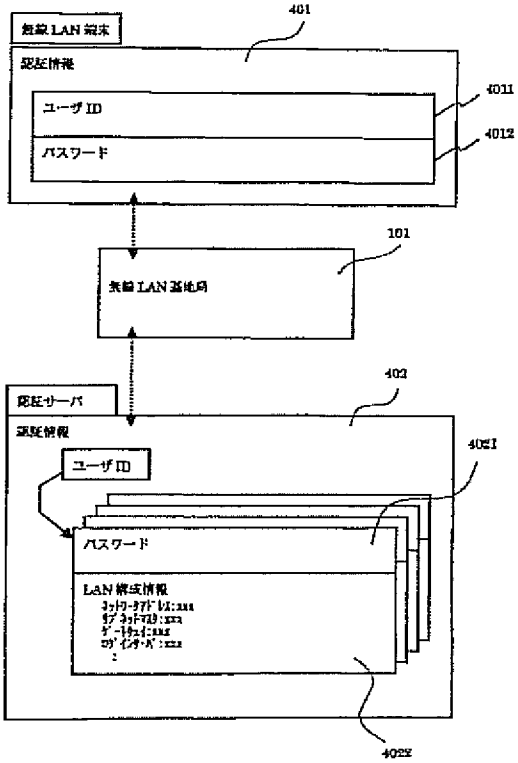
【図2】


104A,104B
無線 LAN 端末
101
無線 LAN 基地局
1041
送受信アンテナ
演算処理装置
1042
LAN 構成情報
設定領域
認証情報
1043
106A

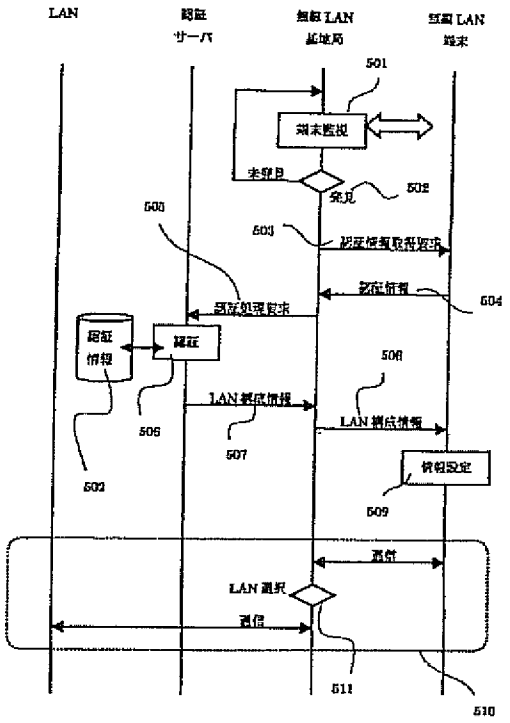
【図3】


101
1011
1012
1015
無線 LAN 基地局
処理制御装置
LAN 通信
交換機構
認証制御
機構
1014
LAN 送受信
アンテナ
認証サーバ
接続インタフェース
端末送受信
アンテナ
1013
1016

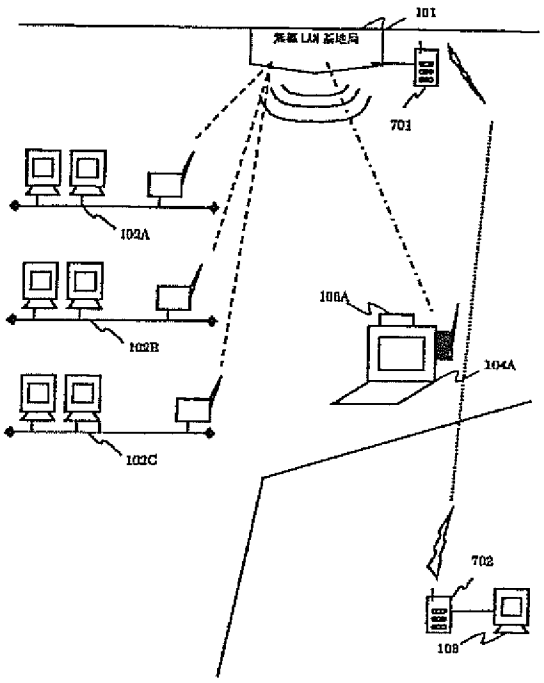
【図4】


無線 LAN 端末
401
認証情報
ユーザ ID
4011
パスワード
4012
101
無線 LAN 基地局
認証サーバ
402
認証情報
ユーザ ID
4021
パスワード
LAN 構成情報
4022

［図５］



［図７］



フロントページの続き

(72)発明者　高橋　宏彰
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウエアエンジニアリング株式会
社内

Ｆターム(参考)　5K033 AA08 AA09 CB01 DA01 DA19
DB20 EA03 EA07 EC01 EC02
EC03